Amendments to the Claims

1. (currently amended) A method comprising the following steps carried out responsive to operation of at least one computer:

   (a)   emitting radiation from at least one radiation emitting device of an automated banking machine, wherein the automated banking machine includes a user interface and a cash dispenser;

   (b)   sensing radiation emitted in (a);

   (c)   capturing first image data corresponding to the user interface;

   (d)   storing the first image data;

   (e)   subsequent to (c), determining that a person is in proximity to the user interface;

   (f)   subsequent to (e), determining that a person is not in proximity to the user interface;

   (g)   responsive to (f), capturing second image data corresponding to the user interface;

(h)   comparing the second image data captured in (g) and the first image data captured in (c), wherein the comparing includes a topographical comparison;

(i)   responsive to (h) resulting in met topographical differences, executing a sequence of actions including:

   (i1)   emitting radiation from the at least one radiation emitting device;

   (i2)   sensing radiation emitted in (i1);

   (i3)   comparing the radiation sensed in (i2) with the radiation sensed in (b);

(j)   responsive to (i3) resulting in met sensed radiation differences, determining that the machine has a fraud condition corresponding to installation of an unauthorized device adjacent the user interface; and

(k)   responsive to a determination in (j) of the fraud condition, sending captured image data including at least the second image data, through a network to enable remote confirmation of an unauthorized device being adjacent the user interface

(a)   ~~sensing at least one condition at a user interface of an automated banking machine including a cash dispenser;~~

(b)   ~~determining through operation of at least one computer in operative connection with the banking machine if the at least one condition sensed in (a) corresponds to installation of a fraud device in connection with the user interface of the machine;~~

(c)   ~~responsive to determination in (b) that the at least one condition corresponds to installation of a fraud device, generating at least one message through operation of the at least one computer.~~

2. (currently amended) The method according to claim 1 wherein (a) ~~includes~~ and (i1) include emitting radiation from at least one radiation emitting device adjacent a card reader slot on the user interface, and wherein (b) and (i2) include sensing ~~a change in~~ at least one property of radiation with ~~a~~ at least one sensor adjacent ~~a~~ the card reader slot ~~on the user interface emitted from a radiation emitter adjacent the card reader slot~~.

3. (canceled)

4. (currently amended) ~~The method according to claim 1 wherein (a) includes sensing~~ A method comprising the following steps carried out responsive to operation of at least one computer:

(a)   emitting radiation from at least one radiation emitting device of an automated

- 4 -

banking machine, wherein the automated banking machine includes a user

interface and a cash dispenser;

(b)   sensing radiation emitted in (a);

(c)   determining that a person is in proximity to the user interface for an extended time

without the person attempting a transaction ~~at the banking~~ with the machine;

(d)   responsive to (c), executing a sequence of actions including:

(d1)   emitting radiation from the at least one radiation emitting device;

(d2)   sensing radiation emitted in (d1);

(d3)   comparing the radiation sensed in (d2) and the radiation sensed in (b);

(e)   responsive to (d3) resulting in met sensed radiation differences,

(e1)   determining that the machine has a fraud condition corresponding to

installation of an unauthorized device adjacent the user interface;

(e2)   obtaining image data corresponding to the user interface; and

- 5 -

(f)   <u>responsive to a determination in (e1) of the fraud condition, sending image data</u>

<u>obtained in (e2) through a network to enable remote confirmation of an</u>

<u>unauthorized device being adjacent the user interface</u>.

5. (currently amended) The method according to claim 1 wherein <u>(h)</u> ~~(a)~~ includes ~~capturing~~

~~image data corresponding to at least a portion of the user interface and~~ detecting a change in

image data corresponding to at least a portion of the user interface.

6-8. (canceled)

9. (currently amended) ~~The method according to claim 8 wherein (a) further includes sensing~~ <u>A</u>

<u>method comprising the following steps carried out responsive to operation of at least one</u>

<u>computer:</u>

     (a)   <u>emitting radiation from at least one radiation emitting device of an automated</u>

<u>banking machine, wherein the automated banking machine includes a user</u>

<u>interface and a cash dispenser;</u>

     (b)   <u>sensing radiation emitted in (a);</u>

     (c)   <u>determining</u> that the machine delivered a receipt to each of a plurality of

sequential users of the ~~banking~~ machine and that each of the sequential users did

not take the respective receipt;

(d)   responsive to (c), executing a sequence of actions including:

(d1)   emitting radiation from the at least one radiation emitting device;

(d2)   sensing radiation emitted in (d1);

(d3)   comparing the radiation sensed in (d2) with the radiation sensed in (b);

(e)   responsive to (d3) resulting in met sensed radiation differences,

(e1)   determining that the machine has a fraud condition corresponding to

installation of an unauthorized device adjacent the user interface;

(e2)   obtaining image data corresponding to the user interface; and

(f)   responsive to a determination in (e1) of the fraud condition, sending image data

obtained in (e2) through a network to enable remote confirmation of an

unauthorized device being adjacent the user interface.

10-11. (canceled)

12. (currently amended) The method according to claim 5 ~~and further comprising~~ wherein (e) includes sensing a transaction ~~when transactions are~~ conducted at the machine ~~, wherein (a) includes comparing image data for at least a portion of the user interface corresponding to different times when transactions are not being conducted at the machine~~.

13. (currently amended) The method according to claim 5 ~~wherein (c) includes~~ and further comprising:

> (l)   responsive to (j), generating a message; ~~corresponding to at least one image of at least a portion of the user interface~~

> wherein (k) includes sending the message through the network.

14. (currently amended) The method according to claim 5 and further comprising:

> (l)   storing data corresponding to a plurality of actions comprising ~~a~~ the sequence in at least one data store; ~~in operative connection with the at least one computer, wherein the at least one computer is operative to execute~~

> wherein (i) includes executing the sequence responsive to a triggering event ~~, and wherein determining that the at least one condition corresponds~~ corresponding to installation of a

- 8 -

~~fraud~~ <u>an unauthorized</u> device ~~comprises the triggering event~~, and <u>wherein</u> the sequence

includes ~~generating the~~ <u>sending</u> at least one message <u>through the network</u>.

15-27. (canceled)